Premiers à la pelle !

Isabelle Dubois

27/05/2023

Laboratoire Institut Elie Cartan de Lorraine - Metz - Université de Lorraine

Pour bien démarrer

Nombres entiers et divisibilité

- 0, 1, 2, 3, 4, ..., 1 000, ..., 1 000 000, ...
  Peut-on écrire la liste de tous les entiers naturels ?

Nombres entiers et divisibilité

- 0, 1, 2, 3, 4, ..., 1 000, ..., 1 000 000, ...
  Peut-on écrire la liste de tous les entiers naturels ?
- Quels sont les entiers qui divisent 12 ?
  Et 35 ? Et 37 ?

Nombres entiers et divisibilité

- 0, 1, 2, 3, 4, ..., 1 000, ..., 1 000 000, ...
  Peut-on écrire la liste de tous les entiers naturels ?
- Quels sont les entiers qui divisent 12 ?
  Et 35 ? Et 37 ?
- Quel est le résultat de la division euclidienne de 12 par 4 ?
  (c'est la "division chez les entiers")
  Par 5 ?

Nombres entiers et divisibilité

- 0, 1, 2, 3, 4, ..., 1 000, ..., 1 000 000, ...
  Peut-on écrire la liste de tous les entiers naturels ?
- Quels sont les entiers qui divisent 12 ?
  Et 35 ? Et 37 ?
- Quel est le résultat de la division euclidienne de 12 par 4 ?
  (c'est la "division chez les entiers")
  Par 5 ?
- Comment reconnaît-on qu'un entier a est divisible par un entier b à l'aide de la division euclidienne de a par b ?

Nombres premiers

- Qu'est-ce qu'un nombre premier ?

Nombres premiers

- Qu'est-ce qu'un nombre premier ?
- Le nombre 0 est-il un nombre premier ?
  Et 1 ?

Nombres premiers

- Qu'est-ce qu'un nombre premier ?
- Le nombre 0 est-il un nombre premier ?
  Et 1 ?
- Donner la liste de tous les nombres premiers inférieurs ou égaux à 12.

A garder en tête pour la suite

Nombre premier

Un nombre premier est un nombre entier qui est divisible par exactement deux entiers : 1 et lui-même.

Les 10 premiers nombres premiers sont :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Quels sont les nombres premiers pairs ?

Peut-on dresser la liste de tous les nombres premiers ?

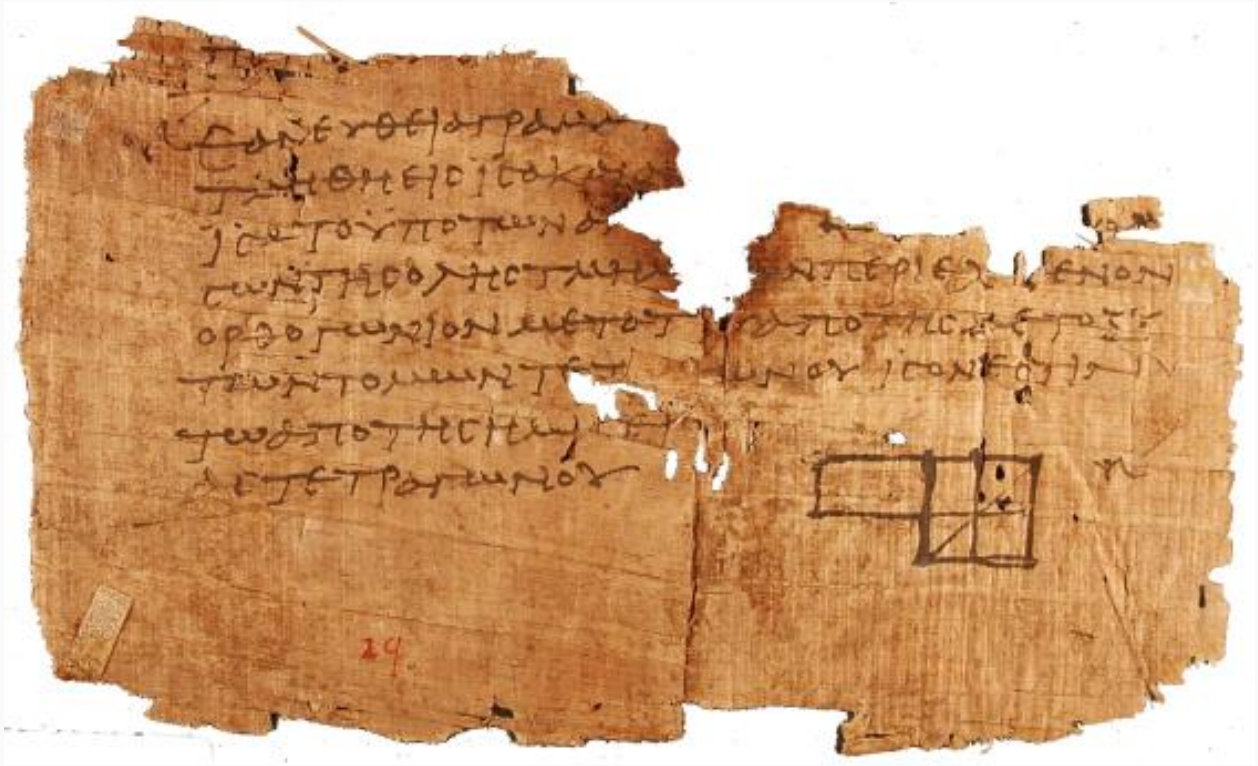
Théorème d'Euclide

Théorème d'Euclide

Idée d'Euclide

Euclide

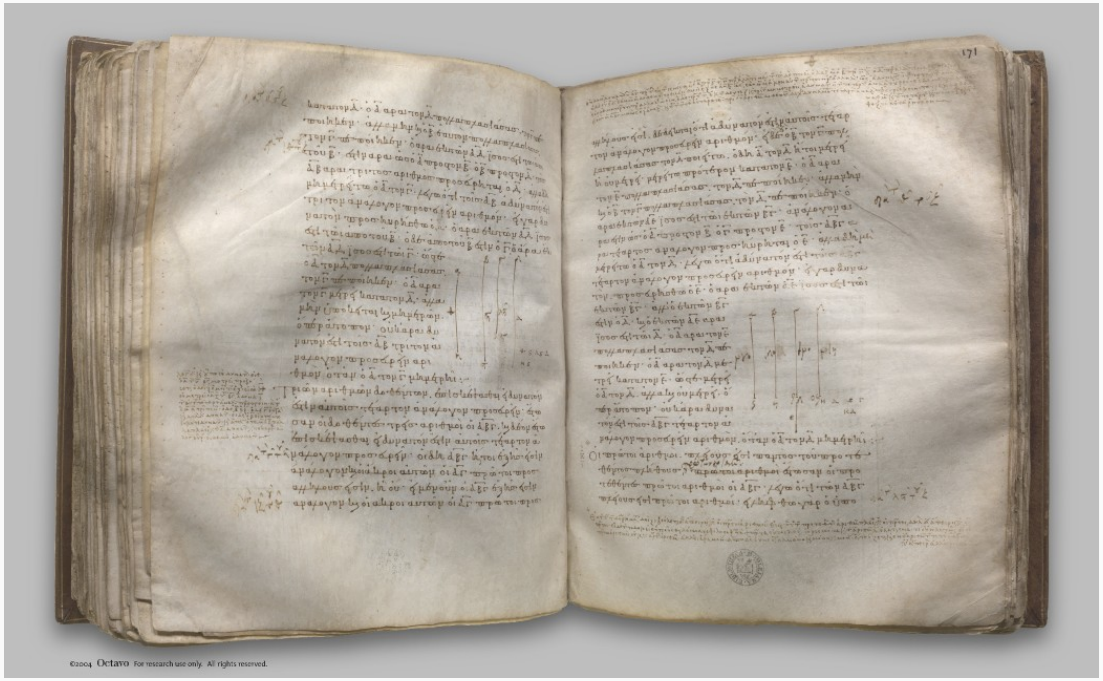
Tout commence par les écrits d'Euclide vers 300 avant J.C.



Un fragment du plus vieux papyrus contenant les travaux d'Euclide
Environ 100 av J.C.

Euclide

Dans l'ouvrage "Éléments", Livre IX, la Proposition 20 concerne la quantité de nombres premiers. Plusieurs traductions et interprétations ont été écrites au fil du temps.



C'est ici ! - Un des plus ancien manuscrit daté des "Éléments", écrit en 888 par le clerc Stéphanos

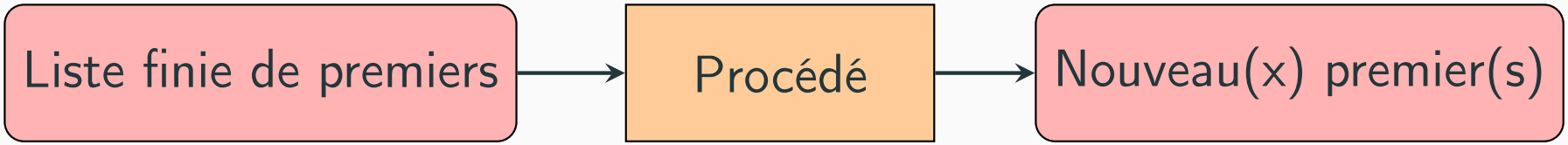
Théorème d'Euclide

Voici une première traduction modernisée de la proposition 20.

Théorème d'Euclide

Il y a plus de nombres premiers que ceux contenus dans n'importe quelle liste finie de nombres premiers.

L'esprit de l'énoncé, et de la démonstration :



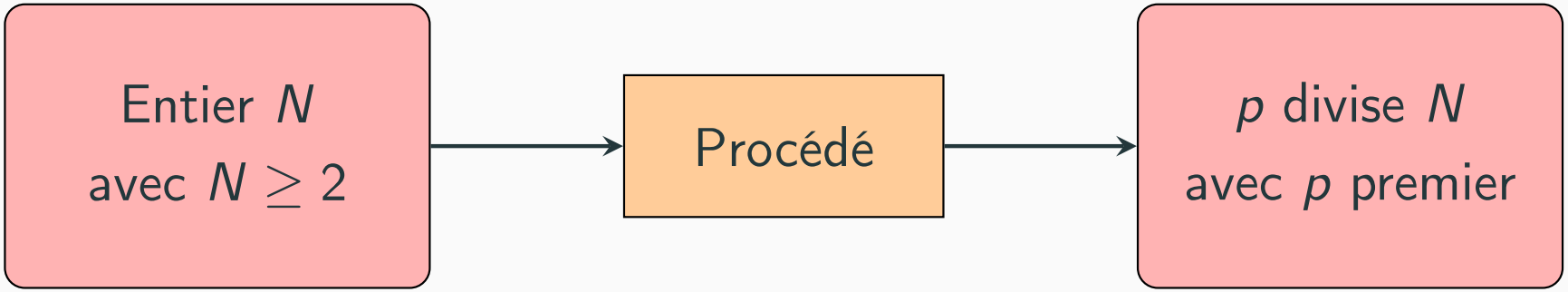
Un ingrédient indispensable

Nous aurons besoin du résultat suivant :

Théorème - Au moins un diviseur premier

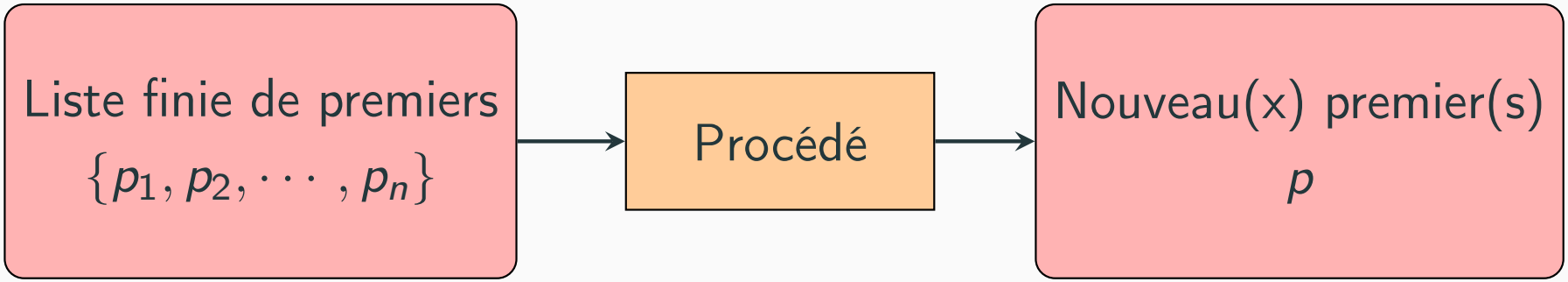
Tout entier supérieur ou égal à 2 est divisible par au moins un nombre premier.

Dit autrement :



Procédé simple : on teste successivement les entiers à partir de 2 ; le premier nombre trouvé qui divise N est un nombre premier.

Procédé du théorème d'Euclide (version modernisée)



On considère $N = p_1 p_2 \cdots p_n + 1$ un entier supérieur ou égal à 2.

On remarque que $\boldsymbol{p_1}$ **ne divise pas** $\boldsymbol{N}$: en effet, dans la division euclidienne de N par p_1, le quotient est $q = p_2 \cdots p_n$ et le reste est $r = 1$.

Même constatation pour les autres premiers p_i de la liste.

Or, **l'entier** N **possède au moins un diviseur** p **qui est un nombre premier.** Ce premier p n'est pas dans la liste donnée, c'est un nouveau premier !

En fait, tout diviseur premier de N **est un nouveau premier**.

Dans la pratique ?

Appliquons le procédé d'Euclide à partir du premier nombre premier. Qu'obtient-on ?

0. *Départ* - On part de la liste $\{2\}$
1. *Première étape* - On considère $N_1 = 2 + 1 = 3$.
   On obtient la liste : $\{2, 3\}$

Dans la pratique ?

Appliquons le procédé d'Euclide à partir du premier nombre premier. Qu'obtient-on ?

0. *Départ* - On part de la liste $\{2\}$
1. *Première étape* - On considère $N_1 = 2 + 1 = 3$.
   On obtient la liste : $\{2, 3\}$
2. *Deuxième étape* - On considère $N_2 = 2 \times 3 + 1 = 7$.
   On obtient la liste : $\{2, 3, 7\}$
3. *Troisième étape* - On considère $N_3 = 2 \times 3 \times 7 + 1 = 43$.
   On obtient la liste : $\{2, 3, 7, 43\}$

Dans la pratique ?

Appliquons le procédé d'Euclide à partir du premier nombre premier. Qu'obtient-on ?

0. *Départ* - On part de la liste $\{2\}$
1. *Première étape* - On considère $N_1 = 2 + 1 = 3$.
   On obtient la liste : $\{2, 3\}$
2. *Deuxième étape* - On considère $N_2 = 2 \times 3 + 1 = 7$.
   On obtient la liste : $\{2, 3, 7\}$
3. *Troisième étape* - On considère $N_3 = 2 \times 3 \times 7 + 1 = 43$.
   On obtient la liste : $\{2, 3, 7, 43\}$
4. *Quatrième étape* - On considère
   $N_4 = 2 \times 3 \times 7 \times 43 + 1 = 1\,807 = 13 \times 139$.
   On obtient la liste : $\{2, 3, 7, 13, 43, 139\}$

Dans la pratique ?

Appliquons le procédé d'Euclide à partir du premier nombre premier. Qu'obtient-on ?

0. *Départ* - On part de la liste $\{2\}$
1. *Première étape* - On considère $N_1 = 2 + 1 = 3$.
   On obtient la liste : $\{2, 3\}$
2. *Deuxième étape* - On considère $N_2 = 2 \times 3 + 1 = 7$.
   On obtient la liste : $\{2, 3, 7\}$
3. *Troisième étape* - On considère $N_3 = 2 \times 3 \times 7 + 1 = 43$.
   On obtient la liste : $\{2, 3, 7, 43\}$
4. *Quatrième étape* - On considère
   $N_4 = 2 \times 3 \times 7 \times 43 + 1 = 1\,807 = 13 \times 139$.
   On obtient la liste : $\{2, 3, 7, 13, 43, 139\}$
5. *Cinquième étape* - On considère
   $N_5 = 2 \times 3 \times 7 \times 13 \times 43 \times 139 + 1 = 3\,263\,443$.
   On obtient la liste : $\{2, 3, 7, 13, 43, 139, 3\,263\,443\}$

Dans la pratique ?

6. *Sixième étape* - On considère
   $N_6 = 2 \times 3 \times 7 \times 13 \times 43 \times 139 \times 3\,263\,443 + 1$
   $N_6 = 10\,650\,056\,950\,807 = 547 \times 607 \times 1\,033 \times 31\,051$.
   On obtient la liste :
   $\{2, 3, 7, 13, 43, 139, 547, 607, 1\,033, 31\,051, 3\,263\,443\}$

Dans la pratique ?

6. *Sixième étape* - On considère
   $N_6 = 2 \times 3 \times 7 \times 13 \times 43 \times 139 \times 3\,263\,443 + 1$
   $N_6 = 10\,650\,056\,950\,807 = 547 \times 607 \times 1\,033 \times 31\,051$.
   On obtient la liste :
   $\{2, 3, 7, 13, 43, 139, 547, 607, 1\,033, 31\,051, 3\,263\,443\}$
7. *Septième étape* - On considère
   $N_7 = 113\,423\,713\,055\,421\,844\,361\,000\,443$
   $N_7 = 29\,881 \times 67\,003 \times 9\,119\,521 \times 6\,212\,157\,481$.
   On obtient la liste :
   $\{2, 3, 7, 13, 43, 139, 547, 607, 1\,033, 29\,881, 31\,051, 67\,003, 3\,263\,443,$
   $9\,119\,521, 6\,212\,157\,481\}$

Limitations et conjecture

- On obtient très vite de très grands entiers et on ne sait pas forcément trouver leurs diviseurs premiers.
  A l'étape 11 on considère le nombre :
  27392450308603031423410234291674686281194364367580914627947367941608692026226993634332118404582438634929548737283992369758487974306317730580753883429460344956410077034761330476016739454649828385541500213920807
- Un (nouveau) nombre premier qui apparaît à l'étape n ne peut plus apparaître aux étapes suivantes.
- **On conjecture que les entiers N_n que l'on considère ne sont jamais divisibles par le carré d'un nombre premier (ou d'un entier)**. Ainsi, les nouveaux nombres premiers qui décomposent N_n à l'étape n, n'apparaitraient qu'une et une seule fois dans cette décomposition, et donc dans toute décomposition.

Théorème d'Euclide

Euclide modernisé - Infini et absurde

Théorème d'Euclide - Version moderne

De nos jours, on présente le théorème d'Euclide de la façon suivante, où "infini" signifie "qui n'est pas en nombre fini" :

Théorème d'Euclide

L'ensemble des nombres premiers est infini.

L'esprit de la démonstration repose sur un raisonnement par l'absurde :

Démonstration par l'absurde

On suppose que les nombres premiers sont en nombre fini.

Soit $L = \{p_1, p_2, \cdots, p_n\}$ leur liste.

On considère $N = p_1 p_2 \cdots p_n + 1$ entier supérieur ou égal à 2.

Comme déjà vu, les p_i ne divisent pas N.

Or, l'entier N possède au moins un diviseur p qui est un nombre premier.

Ce premier p n'est pas dans la liste L, puisqu'il ne peut pas être un des p_i.

Mais, **c'est impossible**, puisque que l'on a donné la liste de tous les nombres premiers ! ! ? ?

C'est donc qu'ils sont en nombre infini.

Euclide en une seule ligne !

En 2015, S. Northshield propose une démonstration "habillée" du théorème d'Euclide (moderne) en une seule ligne, utilisant la fonction sinus.

En voici une adaptation, accessible (en théorie) à tous !

Pour cela, on a besoin de :

Partie fractionnaire

Soit $\{x\}$ la partie fractionnaire d'un nombre décimal ou réel x.

Si n est un entier, alors $\{n\} = 0$. On a aussi : $\{x + n\} = \{x\}$.

Exemples : $\{1{,}2\} = \{184{,}2\} = 0{,}2$ $\qquad$ $\{\pi\} = 0{,}141\,592\cdots$

Euclide en une ligne ?

Et voici une "démonstration en une seule ligne" :

Si l'ensemble $\mathcal{P}$ des nombres premiers est fini, alors :

$$0 < \prod_{p \in \mathcal{P}} \{\frac{1}{p}\} = \prod_{p \in \mathcal{P}} \{\frac{1}{p}(1 + \prod_{q \in \mathcal{P}} q)\} = 0.$$

où $\prod_{p \in \mathcal{P}}$ signifie "le produit sur tous les nombres premiers p".

Je laisse l'audience méditer sur tout ce qui est "caché" dans cette démonstration, et qu'il s'agit en fait d'une revisitation d'Euclide modernisé.

Nombres premiers entre eux et infinitude des premiers

Nombres premiers entre eux et infinitude des premiers

Nombres premiers entre eux

Nombres premiers *entre eux* ?

Attention : c'est une caractéristique qui concerne (au moins) deux nombres entiers, et pas un nombre solitaire !

Nombres premiers entre eux

Deux nombres entiers sont premiers entre eux lorsqu'ils n'ont qu'un seul diviseur en commun, le nombre 1.

Exemples :

- Les entiers 2 et 3 sont premiers entre eux.
- Les entiers 66 ($= 2 \times 3 \times 11$) et 35 ($= 5 \times 7$) sont premiers entre eux.
- Les entiers 3 216 et 932 211 ne sont pas premiers entre eux : ils sont tous les deux divisibles par 3.
- Deux nombres premiers distincts sont premiers entre eux. Par exemple, 211 et 2011.

Nombres premiers entre eux et infinitude des premiers

Goldbach, Hurwitz et les nombres de Fermat

Pierre de Fermat et ses nombres

Pierre de Fermat (1601-1665),

magistrat et mathématicien amateur français

L'histoire commence en 1640, dans une lettre adressée au mathématicien Bernard Frénicle de Bessy.

Pierre de Fermat y introduit des nombres, que l'on appelle aujourd'hui "nombres de Fermat".

Pierre de Fermat et ses nombres

Nombre de Fermat

Un nombre de Fermat est un entier, noté F_n, de la forme :

$$F_n = 2^{2^n} + 1$$

où n est un nombre entier.

Les premiers nombres de Fermat sont :

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$$

Le premier nombre de Fermat qui n'est pas un nombre premier est :

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

Christian Goldbach et son théorème

Christian Goldbach (1690-1764),

mathématicien et "fonctionnaire" russe

L'histoire continue en Juillet 1730, dans une lettre adressée au mathématicien Leonhard Euler.

Goldbach y démontre que les nombres de Fermat sont premiers entre eux deux à deux.

Théorème de Goldbach

Deux nombres de Fermat distincts sont premiers entre eux.

Pourquoi ? Voici les ingrédients de la preuve :

1. On démontre (par un raisonnement par récurrence) que : $F_{n+1} = F_0 F_1 \cdots F_n + 2$
2. Comme les nombres de Fermat sont impairs, on en déduit : F_{n+1} et $F_0 F_1 \cdots F_n$ sont premiers entre eux.
3. Cela prouve le théorème.

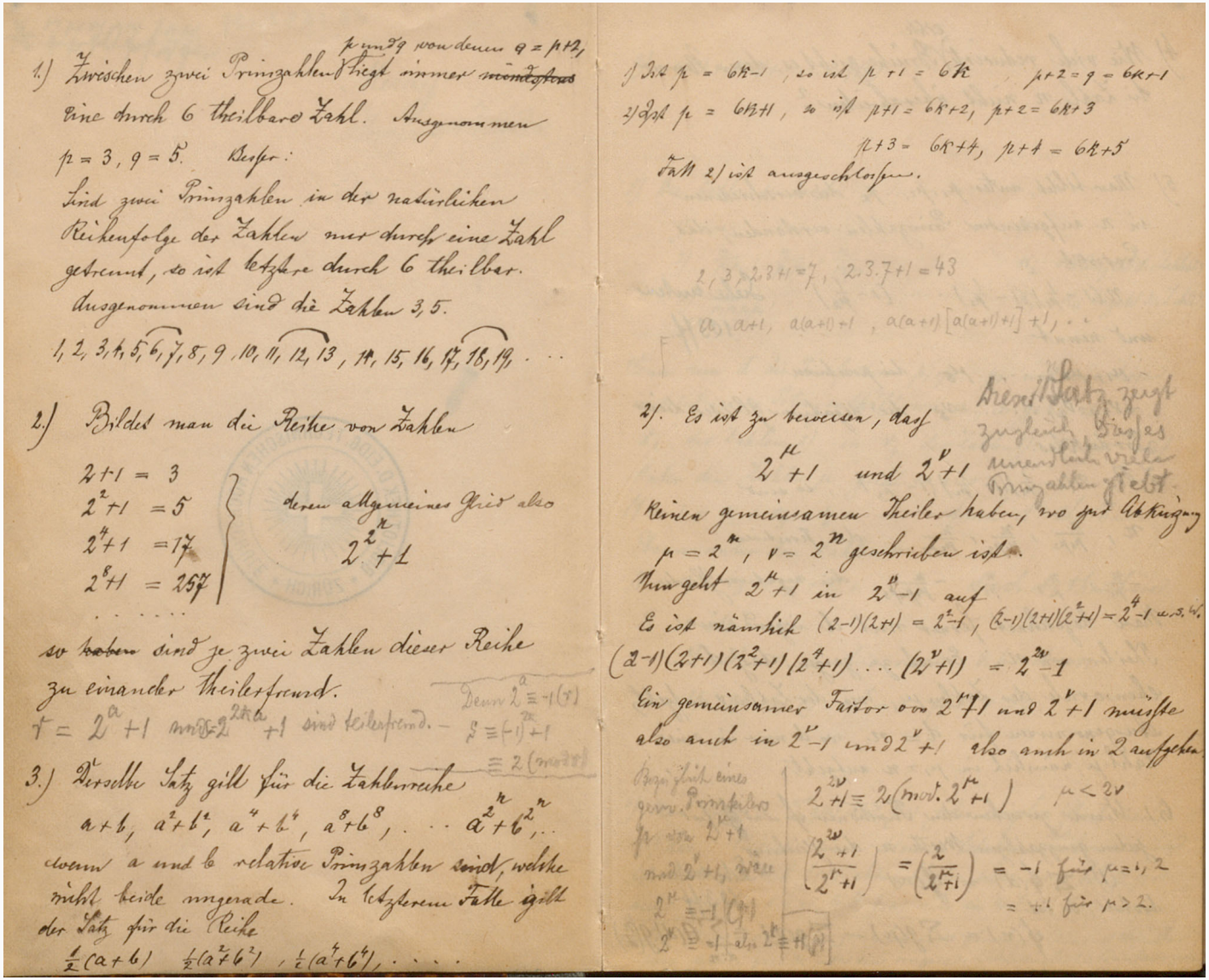
Hurwitz et l'infinitude des premiers

Adolf Hurwitz (1859-1919),

mathématicien allemand

L'histoire s'achève dans un manuscrit d'exercices écrit par Hurwitz entre 1891 à 1918 (publié en 1993 !), intitulé "Übungen zur Zahlentheorie".

Hurwitz et l'infinitude des premiers



1.) Zwischen zwei Primzahlen p und q, von denen $q = p+2$, liegt immer eine durch 6 theilbare Zahl. Ausgenommen $p = 3, q = 5$. Beweis: Sind zwei Primzahlen in der natürlichen Reihenfolge der Zahlen nur durch eine Zahl getrennt, so ist letztere durch 6 theilbar. Ausgenommen sind die Zahlen 3, 5.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, . . .

2.) Bildet man die Reihe von Zahlen

$2+1 = 3$
$2^2+1 = 5$
$2^4+1 = 17$
$2^8+1 = 257$
. . . . .

deren allgemeines Glied also $2^{2^n}+1$

so sind je zwei Zahlen dieser Reihe zu einander theilerfremd.

$r = 2^a+1$ und $2^{2ka}+1$ sind theilerfremd. — Denn $2^a \equiv -1 \pmod r$, $2^{2ka} \equiv (-1)^{2k} \equiv 1 \pmod r$

3.) Derselbe Satz gilt für die Zahlenreihe

$a+b,\ a^2+b^2,\ a^4+b^4,\ a^8+b^8,\ \ldots\ a^{2^n}+b^{2^n},\ldots$

wenn a und b relative Primzahlen sind, welche nicht beide ungerade. In letzterem Falle gilt der Satz für die Reihe

$\frac{1}{2}(a+b),\ \frac{1}{2}(a^2+b^2),\ \frac{1}{2}(a^4+b^4),\ \ldots$

1) Ist $p = 6k-1$, so ist $p+1 = 6k$, $p+2 = q = 6k+1$

2) Ist $p = 6k+1$, so ist $p+1 = 6k+2$, $p+2 = 6k+3$, $p+3 = 6k+4$, $p+4 = 6k+5$

Fall 2) ist ausgeschlossen.

$2, 3, 2.3+1 = 7, 2.3.7+1 = 43$

$a, a+1, a(a+1)+1, a(a+1)[a(a+1)+1]+1, \ldots$

Dieser Satz zeigt zugleich Dass es unendlich viele Primzahlen giebt.

2.) Es ist zu beweisen, dass

$2^\mu+1$ und $2^\nu+1$

keinen gemeinsamen Theiler haben, wo zur Abkürzung $\mu = 2^n$, $\nu = 2^m$ geschrieben ist.

Nun geht $2^\mu+1$ in $2^\nu-1$ auf

Es ist nämlich $(2-1)(2+1) = 2^2-1$, $(2-1)(2+1)(2^2+1) = 2^4-1$ u.s.w.

$(2-1)(2+1)(2^2+1)(2^4+1)\ldots(2^\nu+1) = 2^{2\nu}-1$

Ein gemeinsamer Factor von $2^\mu+1$ und $2^\nu+1$ müsste also auch in $2^\nu-1$ und $2^\nu+1$ also auch in 2 aufgehen

Beispiel eines gem. Factors für $2^\nu+1$ und $2^\mu+1$, wäre $2^\nu \equiv -1$, $2^\nu \equiv +1$

$2^{2\nu}+1 \equiv 2 \pmod{2^\mu+1}$ $\mu < 2\nu$

$\left(\frac{2^{2\nu}+1}{2^\mu+1}\right) = \left(\frac{2}{2^\mu+1}\right) = -1$ für $\mu = 1, 2$

$= +1$ für $\mu > 2$.

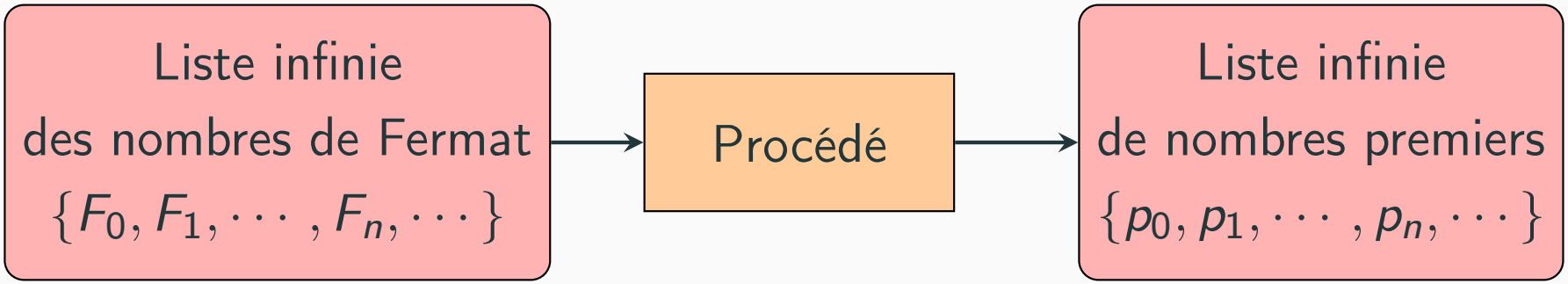
Une annotation affirme : "Ce théorème montre également qu'il existe une infinité de nombres premiers."

Hurwitz et l'infinitude des premiers

Théorème d'Euclide

Les nombres premiers sont en nombre infini.

L'esprit de la démonstration, à la Hurwitz :



Procédé ?

Il suffit, pour chaque entier n, de choisir un nombre premier p_n divisant F_n. Comme les nombres de Fermat sont premiers entre eux deux à deux, tous les p_n sont distincts.

En pratique ?

Quels nombres premiers apparaissent par ce procédé ?

Convenons que pour chaque entier n nous allons choisir le plus petit nombre premier qui divise le nombre F_n.

0. $F_0 = 3$, donc $p_0 = 3$
1. $F_1 = 5$, donc $p_1 = 5$
2. $F_2 = 17$, donc $p_2 = 17$
3. $F_3 = 257$, donc $p_3 = 257$
4. $F_4 = 65\,537$, donc $p_4 = 65\,537$
5. $F_5 = 4\,294\,967\,297$, donc $p_5 = 641$
6. $F_6 = 18\,446\,744\,073\,709\,551\,617$, donc $p_6 = 274\,177$
7. $F_7 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457$, donc $p_7 = 59\,649\,589\,127\,497\,217$

Et après ? Il devient difficile d'aller très loin par ce procédé.

En pratique ? A vous de participer !

Au 22 avril 2023, voici l'état de connaissance sur la factorisation des nombres de Fermat en produit de nombres premiers :

- Seuls les nombres F_0 à F_{11} sont complètement factorisés.
- On a découvert 362 nombres premiers divisant un nombre de Fermat.
- Le dernier a été trouvé le 21 avril 2023 par Gary Gostin. C'est : $713\,828\,860\,473 \times 2^{21438} + 1$. Il divise $F_{1\,436}$.
- Si vous possédez un ordinateur, vous pouvez collaborer à la recherche participative de facteurs premiers des nombres de Fermat et, pourquoi pas, laisser votre nom à la postérité. Pour tout renseignement à ce sujet : fermatsearch.org

Nombres premiers entre eux et infinitude des premiers

Wunderlich et Fibonacci

Wunderlich et les nombres entiers

Marvin Charles Wunderlich (1931-2013) est un mathématicien américain qui s'est intéressé à la théorie des nombres, et en particulier aux méthodes algorithmiques de factorisation de grands entiers en facteurs premiers.

Dans les années 80 il a notamment implémenté un algorithme de factorisation par un procédé de calcul parallèle sur un "Processeur Massivement Parallèle" qui avait été développé par Goodyear Aerospace pour la NASA.

Il n'a apparemment pas factorisé des nombres de Fermat, mais des nombres de la forme $5^n + 1$ et des nombres de Mersenne de la forme $2^n - 1$.

En 1965, il a publié un court article démontrant l'infinitude des nombres premiers qui utilise les nombres de Fibonacci.

Nombres de Fibonacci

Leonardo Fibonacci, mathématicien italien (1170-1250)

Les nombres de Fibonacci sont les nombres entiers f_n définis par :

$f_1 = 1,\ f_2 = 1,\ f_3 = f_1 + f_2 = 2,\ f_4 = f_2 + f_3 = 3,\ f_5 = f_3 + f_4 = 5,$

$f_6 = f_4 + f_5 = 8,\ f_7 = f_5 + f_6 = 13,\ \ldots,\ f_n = f_{n-2} + f_{n-1},\ \ldots$

Wunderlich et les nombres de Fibonacci

En se basant sur la propriété (bien connue) :

Propriété des nombres de Fibonacci

Si les entiers m et n sont premiers entre eux, alors les nombres de Fibonacci f_m et f_n sont premiers entre eux.

Wunderlich, en 1965, déduit :

Théorème d'Euclide

L'ensemble des nombres premiers est infini.

en faisant un raisonnement par l'absurde :

Wunderlich et les nombres de Fibonacci

Soit $\{p_1 = 2, p_2 = 3, \cdots, p_{12} = 37, \cdots, p_n\}$ la liste des nombres premiers, **supposée finie de taille n**.

On considère alors la liste $\{f_{p_1}, f_{p_2}, \cdots, f_{p_n}\}$.

Elle contient n nombres de Fibonacci différents et premiers entre eux deux à deux, car leurs indices le sont.

On remarque que $f_{p_1} = f_2 = 1$, et les suivants vérifient : $f_{p_i} \geq 2$.

Ainsi, les nombres premiers qui divisent les f_{p_i} (sauf f_2), sont tous différents : il y en a donc au moins $n - 1$.

Or, $f_{37} = 24\,157\,817 = 73 \times 149 \times 2221$. **Cela fait donc au moins $n + 1$ nombres premiers existant.**

Mais, c'est impossible, puisque la liste de tous les nombres premiers contient n nombres ! ! ? ? C'est donc qu'ils sont en nombre infini.

Nombres de Fibonacci et nombres premiers

Finalement, quels sont les nombres premiers cachés dans les nombres de Fibonacci ? Tous !

Théorème - Nombres premiers et nombres de Fibonacci

Tout nombre premier divise une infinité de nombres de Fibonacci.

Un nombre premier p quelconque divise l'un des nombres de Fibonacci suivant : f_{p-1}, f_p, ou f_{p+1}.

Question ouverte

Existe-t-il une infinité de nombres de Fibonacci qui sont des nombres premiers ? On ne sait pas !

Le plus grand nombre premier de Fibonacci connu est $f_{148\,091}$ (Août 2021, Facq, Asuncion, Allombert).

Le plus grand nombre probablement premier de Fibonacci connu est $f_{6\,530\,879}$ (Août 2022, Propper).

Dirichlet et premiers en progression arithmétique

Dirichlet et premiers en progression arithmétique

N'y aurait-il pas des motifs ?

Observons

En regardant une liste des premiers nombres premiers, voici un début de liste de nombres premiers se terminant par :

- 1 : 11, 31, 41, 61, 71, 101, 131, 151, 181, 191, 211...
- 3 : 3, 13, 23, 43, 53, 73, 83, 103, 113, 163, 173...
- 7 : 7, 17, 37, 47, 67, 97, 107, 127, 137, 157, 167...
- 9 : 19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229...
- 11 : 11, 211, 311, 811, 911, 1511, 1811, 2011...
- 21 : 421, 521, 821, 1021, 1321, 1621, 1721, 2221...
- 37 : 37, 137, 337, 937, 1237, 1637, 2137, 2237...
- 39 : 139, 239, 439, 739, 839, 1039, 1439, 2039...
- 1013 : 1013, 21013, 31013, 81013, 121013, 151013, 241013, 261013...

Ces listes sont-elles infinies ?

Réponse - Théorème de Dirichlet

OUI ! ! Cela provient du :

Théorème de Dirichlet (1837)

Soit a et b deux nombres entiers premiers entre eux.

Il existe une infinité de nombres premiers de la forme $a \times n + b$, où n est un entier.

Exemples

- Avec $a = 10$ et $b = 1$ (ou 3, ou 7, ou 9) : il existe une infinité de nombres premiers se terminant par le chiffre unité b.
- Avec $a = 100$ et $b = 11$ (ou 21, ou 37, ou 39) : il existe une infinité de nombres premiers se terminant par le nombre à deux chiffres b.
- Avec $a = 10000$ et $b = 1013$: il existe une infinité de nombres premiers se terminant par 1013.

Démonstration classique - Euler et Dirichlet

La démonstration du théorème de Dirichlet fait appel à des outils sophistiqués des mathématiques, dépassant le cadre scolaire.

Euler démontre le cas particulier des premiers de la forme $a \times n + 1$ en 1775, et Dirichlet le cas général en 1837.

Leonhard Euler, mathématicien et physicien suisse (1707-1783)

Johann Peter Gustav Lejeune Dirichlet, mathématicien prussien (1805-1859)

Dirichlet et premiers en progression arithmétique

Cas particuliers "à la Euclide"

Premiers de la forme $4n+1$ ou $4n+3$

Il est possible de démontrer l'infinité de nombres premiers de la forme $4n+1$ ou $4n+3$ "à la Euclide".

Pourquoi considérer ces deux écritures ?

Conséquence de la division euclidienne par 4

Tout nombre entier N s'écrit sous la forme :

$$4n, \text{ ou bien } 4n+1, \text{ ou bien } 4n+2, \text{ ou bien } 4n+3,$$

où n est un nombre entier.

En effet, en effectuant la division euclidienne de N par 4, on trouve un quotient entier, c'est n, et un reste qui vaut 0, 1, 2, ou 3.

- Quels sont ceux qui sont pairs ? impairs ?
- Les nombres premiers sont-ils pairs ? impairs ?

Premiers de la forme $4n+1$ ou $4n+3$

Nous aurons besoin du résultat suivant :

Propriété utile

Le produit de deux nombres de la forme $4n+1$ est de la forme $4n+1$.

En effet,

$$(4n+1)(4m+1) = 4(4nm+n+m)+1$$

qui est bien de la forme $4N+1$, avec N un entier naturel.

Exemple : $5 \times 9 = 45 = 44+1$

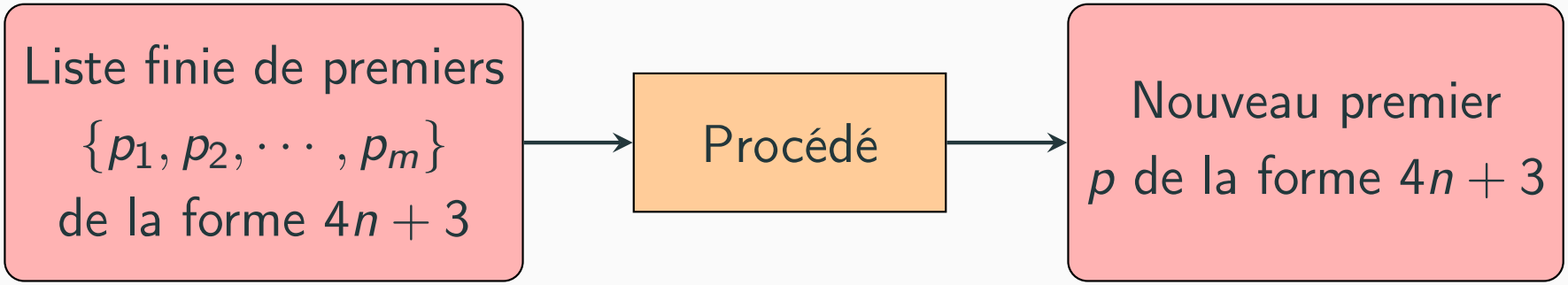
Attention : c'est faux pour les nombres de la forme $4n+3$.

Par exemple, $3 \times 7 = 21 = 20+1$.

Infinité de premiers de la forme $4n+3$

Il existe au moins un premier de la forme $4n+3$, par exemple 3.

Et il existe un procédé pour obtenir de nouveaux tels premiers :



On considère $N = 4p_1p_2\cdots p_m - 1 = 4(p_1p_2\cdots p_m - 1) + 3$.

Comme N est impair, ses diviseurs le sont aussi.

Si tous les diviseurs premiers de N étaient de la forme $4n+1$, alors N le serait aussi, ce qui n'est pas.

Donc, on peut trouver un premier p qui divise N et de la forme $4n+3$. De plus, on constate qu'il est nouveau.

Infinité de premiers de la forme $4n+3$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 3.

0. *Départ* - On part de la liste $\{3\}$
1. *Première étape* - On considère $N_1 = 4 \times 3 - 1 = 11$.
   On obtient la liste : $\{3, 11\}$

Infinité de premiers de la forme $4n+3$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 3.

0. *Départ* - On part de la liste $\{3\}$
1. *Première étape* - On considère $N_1 = 4 \times 3 - 1 = 11$.
   On obtient la liste : $\{3, 11\}$
2. *Deuxième étape* - On considère $N_2 = 4 \times 3 \times 11 - 1 = 131$.
   On obtient la liste : $\{3, 11, 131\}$
3. *Troisième étape* - On considère
   $N_3 = 4 \times 3 \times 11 \times 131 - 1 = 17\,291$.
   On obtient la liste : $\{3, 11, 131, 17\,291\}$

Infinité de premiers de la forme $4n+3$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 3.

0. *Départ* - On part de la liste $\{3\}$
1. *Première étape* - On considère $N_1 = 4 \times 3 - 1 = 11$.
   On obtient la liste : $\{3, 11\}$
2. *Deuxième étape* - On considère $N_2 = 4 \times 3 \times 11 - 1 = 131$.
   On obtient la liste : $\{3, 11, 131\}$
3. *Troisième étape* - On considère
   $N_3 = 4 \times 3 \times 11 \times 131 - 1 = 17\,291$.
   On obtient la liste : $\{3, 11, 131, 17\,291\}$
4. *Quatrième étape* - On considère
   $N_4 = 4 \times 3 \times 11 \times 131 \times 17\,291 - 1 = 298\,995\,971$.
   On obtient la liste : $\{3, 11, 131, 17\,291, 298\,995\,971\}$

Infinité de premiers de la forme $4n+3$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 3.

0. *Départ* - On part de la liste $\{3\}$
1. *Première étape* - On considère $N_1 = 4 \times 3 - 1 = 11$.
   On obtient la liste : $\{3, 11\}$
2. *Deuxième étape* - On considère $N_2 = 4 \times 3 \times 11 - 1 = 131$.
   On obtient la liste : $\{3, 11, 131\}$
3. *Troisième étape* - On considère
   $N_3 = 4 \times 3 \times 11 \times 131 - 1 = 17\,291$.
   On obtient la liste : $\{3, 11, 131, 17\,291\}$
4. *Quatrième étape* - On considère
   $N_4 = 4 \times 3 \times 11 \times 131 \times 17\,291 - 1 = 298\,995\,971$.
   On obtient la liste : $\{3, 11, 131, 17\,291, 298\,995\,971\}$
5. *Cinquième étape* - On considère
   $N_5 = 4 \times 3 \times 11 \times 131 \times 17\,291 \times 298\,995\,971 - 1 =$
   $89\,398\,590\,973\,228\,811 = 8\,779 \times 10\,079 \times 1\,010\,341\,471$.
   On obtient la liste : $\{3, 11, 131, 17\,291, 298\,995\,971, 8\,779\}$

Infinité de premiers de la forme $4n + 3$ - Dans la pratique

Au bout de 13 étapes, on obtient la liste suivante :

$$\{3,\ 11,\ 131,\ 17\,291,\ 298\,995\,971,\ 8\,779,$$

$$594\,359,\ 59,\ 151,\ 983,\ 19,$$

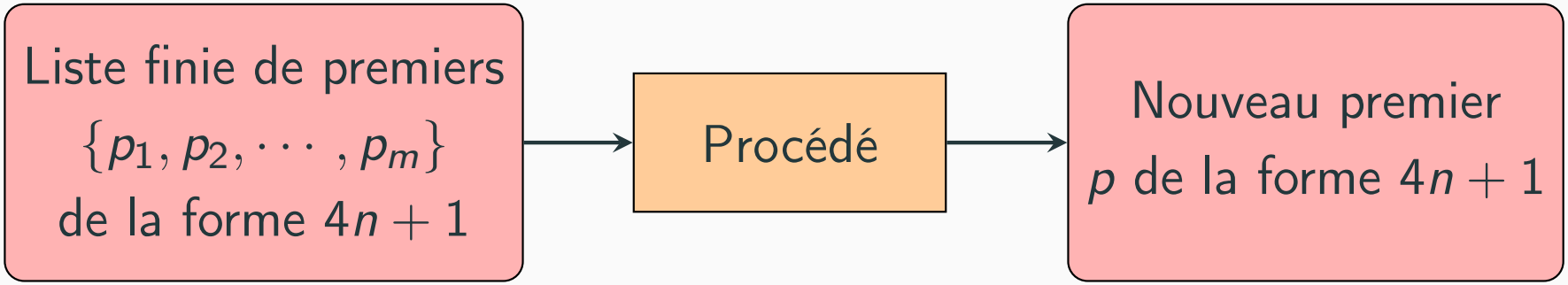
$$38\,851\,089\,348\,584\,904\,271\,503\,421\,339,$$

$$2\,359\,886\,893\,253\,830\,912\,337\,243\,172\,544\,609\,142\,020\,402\,559\,023\}$$

Infinité de premiers de la forme $4n+1$

Il existe au moins un premier de la forme $4n+1$, par exemple 5.

Et il existe un procédé pour obtenir de nouveaux tels premiers :



On considère $N = 4(p_1 p_2 \cdots p_m)^2 + 1$.

Soit p un nombre premier (impair) qui divise N. On a ainsi une égalité du type : $(2p_1 p_2 \cdots p_m)^2 = -1 + kp$.

Alors, on peut montrer (mais cela demande un peu de travail) que $\dfrac{p-1}{2}$ est un nombre pair.

On en déduit que tout premier p qui divise N est de la forme $4n+1$. De plus, on constate qu'un tel premier est nouveau.

Infinité de premiers de la forme $4n+1$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 5.

0. *Départ* - On part de la liste $\{5\}$
1. *Première étape* - On considère $N_1 = 4 \times 5^2 + 1 = 101$.
   On obtient la liste : $\{5, 101\}$

Infinité de premiers de la forme $4n+1$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 5.

0. *Départ* - On part de la liste $\{5\}$
1. *Première étape* - On considère $N_1 = 4 \times 5^2 + 1 = 101$.
   On obtient la liste : $\{5, 101\}$
2. *Deuxième étape* - On considère
   $N_2 = 4 \times (5 \times 101)^2 + 1 = 1\,020\,101$.
   On obtient la liste : $\{5, 101, 1\,020\,101\}$
3. *Troisième étape* - On considère
   $N_3 = 4 \times (5 \times 101 \times 1\,020\,101)^2 + 1 =$
   $1\,061\,522\,231\,810\,040\,101 = 53 \times 1\,613 \times 12\,417\,062\,216\,309$.
   On obtient la liste : $\{5, 101, 1\,020\,101, 53\}$

Infinité de premiers de la forme $4n+1$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 5.

0. *Départ* - On part de la liste $\{5\}$
1. *Première étape* - On considère $N_1 = 4 \times 5^2 + 1 = 101$.
   On obtient la liste : $\{5, 101\}$
2. *Deuxième étape* - On considère
   $N_2 = 4 \times (5 \times 101)^2 + 1 = 1\,020\,101$.
   On obtient la liste : $\{5, 101, 1\,020\,101\}$
3. *Troisième étape* - On considère
   $N_3 = 4 \times (5 \times 101 \times 1\,020\,101)^2 + 1 =$
   $1\,061\,522\,231\,810\,040\,101 = 53 \times 1\,613 \times 12\,417\,062\,216\,309$.
   On obtient la liste : $\{5, 101, 1\,020\,101, 53\}$
4. *Quatrième étape* - On considère
   $N_4 = 29 \times 137 \times 8\,143\,721 \times 92\,159\,345\,497$.
   On obtient la liste : $\{5, 101, 1\,020\,101, 53, 29\}$

Infinité de premiers de la forme $4n+1$ - Dans la pratique

Appliquons ce procédé à partir du nombre premier 5.

0. *Départ* - On part de la liste $\{5\}$
1. *Première étape* - On considère $N_1 = 4 \times 5^2 + 1 = 101$.
   On obtient la liste : $\{5, 101\}$
2. *Deuxième étape* - On considère
   $N_2 = 4 \times (5 \times 101)^2 + 1 = 1\,020\,101$.
   On obtient la liste : $\{5, 101, 1\,020\,101\}$
3. *Troisième étape* - On considère
   $N_3 = 4 \times (5 \times 101 \times 1\,020\,101)^2 + 1 =$
   $1\,061\,522\,231\,810\,040\,101 = 53 \times 1\,613 \times 12\,417\,062\,216\,309$.
   On obtient la liste : $\{5, 101, 1\,020\,101, 53\}$
4. *Quatrième étape* - On considère
   $N_4 = 29 \times 137 \times 8\,143\,721 \times 92\,159\,345\,497$.
   On obtient la liste : $\{5, 101, 1\,020\,101, 53, 29\}$
5. *Cinquième étape* - On considère
   $N_5 = 2\,507\,707\,213\,238\,852\,620\,996\,901$.
   On obtient la liste :
   $\{5, 101, 1\,020\,101, 53, 29, 2\,507\,707\,213\,238\,852\,620\,996\,901\}$

Infinité de premiers de la forme $4n+1$ - Dans la pratique

Au bout de 13 étapes, on obtient la liste suivante :

$$\{5,\ 101,\ 1\,020\,101,\ 53,\ 29,$$

$$2\,507\,707\,213\,238\,852\,620\,996\,901,$$

$$449,\ 13,\ 8\,693,\ 1\,997,\ 6\,029,\ 61,\ 3\,181\,837\}$$

Limitations des preuves "à la Euclide"

On peut se demander si on peut ainsi démontrer le théorème de Dirichlet "à la Euclide" dans tous les cas. Il n'en est rien comme le dit ce résultat :

Théorème de possibilité/impossibilté de I. Schur (1912) et M.R. Murty (1988)

Soient a et b deux nombres premiers entre eux.

Il existe une démonstration *"à la Euclide"* de l'infinitude des nombres premiers de la forme $a \times n + b$ si et seulement si l'entier b^2 est de la forme $a \times n + 1$.

Exemples :

- Si $b = \pm 1$, il existe toujours une telle démonstration.
- Si $a = 6$ et $b = 5$, il existe une telle démonstration.
- Si $a = 10$ et $b = 1$, 5, 7 ou 9, il en existe une.
- Si $a = 100$ et $b = 11$, 21, 37, ou 39, il n'en existe pas.

Ouvertures et Conjectures

Conjecture de Goldbach(-Euler)

Revenons aux échanges épistolaires de Goldbach et Euler, et l'année 1742. D'une suggestion de Goldbach, et de la réponse donnée par Euler, est née une célèbre conjecture :

Conjecture de Goldbach (1742)

Tout nombre entier pair supérieur ou égal à 4 est somme de deux nombres premiers.

Exemples :

$56 = 3 + 53 = 13 + 43 = 19 + 37$

$2024 = 7 + 2017 = 13 + 2011 = 31 + 1993 = 37 + 1987 = ...$

Cette conjecture n'est toujours pas démontrée !

Nombres premiers de Sophie Germain

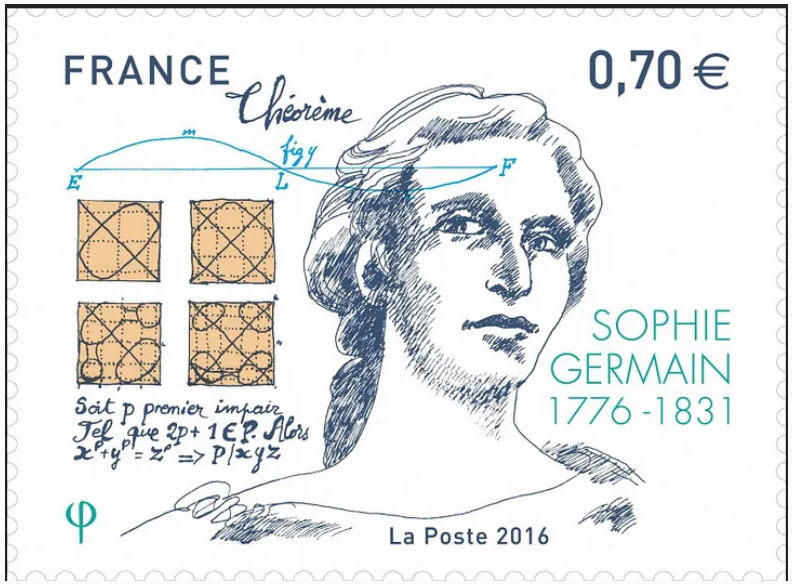
Sophie Germain (1776-1831),

pseudo Antoine Auguste Leblanc (1794-1807),

mathématicienne et physcienne autoditacte, philosophe française

Célèbre pour ses travaux concernant l'étude des surfaces élastiques, et ses apports en théorie des nombres, notamment en lien avec le grand théorème de Fermat.

Nombres premiers de Sophie Germain



Timbre en l'honneur de Sophie Germain

Nombres premiers de Sophie Germain

Un nombre premier p est un premier de Sophie Germain si $2p + 1$ est lui aussi un nombre premier.

Exemples : Les premiers 2, 3, 5, 11, 23, 29, 41, 53, 83, 89 sont tous les premiers de Sophie Germain inférieurs à 100.

Nombres premiers de Sophie Germain

- Ils ont joué un rôle dans la résolution du grand théorème de Fermat.

Théorème de Sophie Germain (1825 ?)

Soit p un nombre premier de Sophie Germain.
Alors, il n'existe pas de nombres entiers non nuls x, y et z, et non divisibles par p, tels que : $x^p + y^p = z^p$.

- On conjecture qu'il existe une infinité de nombres premiers de Sophie Germain.
  Record : Le plus grand tel premier connu est le nombre (possédant 388 342 chiffres), découvert en février 2016 : $2\,618\,163\,402\,417 \cdot 2^{1290000} - 1$
- En cryptographie, les premiers de Sophie Germain sont des nombres premiers dits "sûrs" et sont utilisés dans certains protocoles.

Gauss, apprenant la supercherie, écrit à Sophie Germain

Comment vous décrire mon admiration et mon étonnement de voir mon estimé correspondant Monsieur Le Blanc se transformer en ce fameux personnage qui me donne un brillant exemple de ce que j'aurais du mal à croire. Le goût des sciences abstraites en général et plus particulièrement des mystères des nombres est extrêmement rare. Les charmes de cette sublime science ne se révèlent qu'à ceux qui ont le courage de l'explorer en profondeur. Mais quand une personne du sexe qui, du fait de nos coutumes et préjugés, doit surmonter plus de difficultés que les hommes pour se familiariser avec ces épineuses questions, réussit néanmoins à dépasser ces obstacles et à appréhender leur partie la plus obscure, alors elle doit sans aucun doute posséder un noble courage, des talents extraordinaires et un esprit supérieur. De fait, rien de plus flatteur et moins équivoque, que la prédilection avec laquelle vous avez honoré cette science, qui a enrichi ma vie de tant de joie, ne pourrait me montrer que ses attraits ne sont pas chimériques.

Lettre du 30 avril 1807,
jour de l'anniversaire de naissance de Gauss

Lettre de Gauss à S. Germain quand il apprend que le pseudo Le Blanc cache une femme.